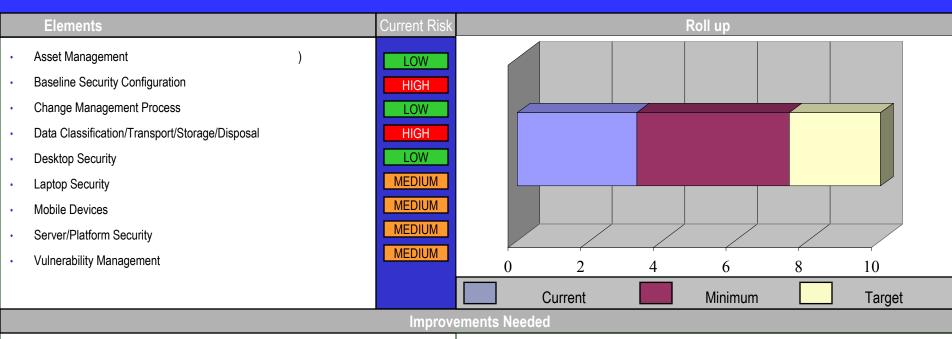
High-level Risk Assessment Summary

Security Policy	Information Risk	Policies, Procedures,					<u> </u>
	Management	Standards, Guidelines	Privacy				
Organizational Security	Organizational Structure	Service Level (SLA) Management					
Asset Classification and Control	Baseline Security		Asset				
	Configuration	Change Management	Management	Desktop Security	Laptop Security	Mobile Device	Server Security
	Data Classification Storage/Transport/Disposal		Vulnerability Management	Wireless			
Personnel Security	Daw Glassification Corag	of transport Bispocal	Incident				
			Response &				
	Awareness Training	Social Engineering	Reporting				
Physical and Environmental	Physical Data Center Security	Desktop Security	Laptop Security	Mobile Devices	Server Security		
Communications and Operations Security	-		Network				Virus
	Backup & Recovery	Email Delivery Architecture	Architecture	Intrusion Detection	Wireless	Secure Communications	Management
		Incident Response &	Event	Instant			
	Auditing and Logging	Reporting	Correlation	Messaging/Peer- Peer Services	Monitoring	Content Filtering	
Access Control	3 33 3	Enterprise Directory	Identity		Role Based Access	Encryption and Digital	
	VPN	Services	Management	Single Sign On	Control	Signatures	
Systems Development &		Encryption and Digital					
Maintenance	Application Security	Signatures					
Business Continuity	Disaster Recovery	Business Continuity					
Compliance	Compliance Program Management						

Domain III - Asset Classification & Controls



Asset Management

- Classify assets by sensitivity and criticality
- Develop and implement asset disposal / re-use plan
- Implement a comprehensive asset inventory

Baseline Security Management

 Define a standardized/updated/automated secure configuration and 'hardened' loadsets for all assets (desktops, laptops, servers, switches, routers, etc.) with auditing and logging enabled

Change Management Process

- Define and implement a formal change management for configuration, application source code etc
- Set up a pilot/test platform for all critical infrastructures (File/Print, data-warehouse, etc.)

Data Classification/Transport/Storage/Disposal

 Develop policy and define technologies for secure storage, transmission and disposal of data

Laptop Security

- Deploy multiple levels of access control like BIOS passwords, Hard disk passwords etc.
- Encryption of sensitive data

Mobile Devices

- Encrypt wireless communications for mobile devices
- Use local encryption and password protection on devices

Vulnerability management

Automated and centralized vulnerability management

Domain VI – Comm. & Operations Security

Current Risl Roll up MEDIUM Auditing and Logging **MEDIUM Email Delivery MEDIUM** Instant Messaging/Peer-peer Services LOW Monitoring **MEDIUM** Content Filtering HIGH Secure Communication HIGH Wireless Incident Response and Reporting LOW **Event Correlation** LOW Backup and Recovery **MEDIUM** Minimum Current Target Network Architecture MEDIUM **Secure Communication** Deploy a universal secure communication mechanisms as opposed to Intrusion Detection **MEDIUM** securé email Virus Detection Wireless HIGH Create a policy and secure new and existing Home wireless networks **Event Correlation** Improvements Needed Develop Event correlation strategy and architecture Auditing and Logging Backup and Recovery Perform standardized & centralized logging- integrated with devices & applications Deploy ability to encrypt backup data Validate backup plans against record retention guidelines **Email Delivery** Internal Network Architecture Redundant content filtering Implement mechanisms to authenticate users prior to obtaining access to Xyz resources (IP, DHCP, DNS, etc.) Instant Messaging/Peer-peer Services Discover and secure IM usage Introduce internal firewalling based on data criticality and sensitivity Consider Proxies and authenticated outbound Internet access Define usage policy **Monitoring** Intrusion Detection Deploy a system to enable centralized real time monitoring across enterprise Deploy both Network and Host Based IDS Virus Detection **Content Filtering** Ensure comprehensive protection from viruses on all gateways and Filter inbound and outbound communications Build in redundancy in delivery/monitoring mechanisms